WE CLAIM:

1. A method for authenticating a client over a network, comprising:

generating a first certificate;

sending the first certificate to a server, wherein the server is configured to store the first certificate;

requesting a second certificate if authentication over the network is requested;

sending the second certificate to the server over the network;

comparing the second certificate to the first certificate at the server, and if the second certificate and the first certificate are substantially the same, authenticating the client.

2. The method of Claim 1, wherein the server is further configured to generate the first certificate.

3. The method of Claim 1, wherein sending the first certificate further comprises using a trusted mechanism selected from at least one of a manual entry of certificate, a secure channel, and a private channel.

4. The method of Claim 3, wherein the trusted mechanism further comprises at least one of the client authenticating to the server, and the client proving ownership of the certificate to the server.

5. The method of Claim 1, wherein the client is further configured to generate the first certificate.

6. The method of Claim 1, wherein a third party Certificate Authority (CA) is configured to generate the first certificate.

7. A method for authenticating a client over a network, comprising:

receiving a certificate from the client over a trusted mechanism;

storing the certificate at a server;

requesting another certificate if authentication is requested;

comparing the other certificate to the stored certificate, and if the other certificate and the stored certificate are substantially the same, authenticating the client.

8. The method of Claim 7, wherein the trusted mechanism further comprises at least one of a manual entry of certificate, a secure channel, and a private channel.

9. The method of Claim 8, wherein the trusted mechanism further comprises at least one of the client authenticating to the server, and the client proving ownership of the certificate to the server.

10. The method of Claim 7, wherein the server is further configured to store and to compare the certificate.

11. The method of Claim 7, wherein the certificate is stored in at least one of a hard disk, a tape disk, and a mass storage device.

12. A method for authenticating a network device over a network, comprising:

generating a certificate;

sending the certificate to another network device, wherein the other network device enables storage of the certificate;

resending the certificate to the other network device; and

if the resent certificate and the stored certificate are substantially the same, receiving authentication.

13. The method of Claim 12, wherein generating the certificate is performed by the other network device.

14. The method of Claim 12, wherein the network device is configured to generate the first certificate.

15. The method of Claim 12, wherein a third party Certificate Authority (CA) is configured to generate the first certificate.

16. An apparatus for authenticating a client over a network, comprising:

a first component configured to receive a first certificate and a second certificate; and

a second component, coupled to the first component, that is configured to perform actions including:

determining if the first certificate and the second certificate are substantially the same; and

if it is determined that the first certificate and the second certificate are substantially the same, authenticating the client associated with the first certificate and the second certificate.

17. The apparatus of Claim 16, wherein the apparatus operates as at least one of a server, a gateway, and a server array.

18. The apparatus of Claim 16, wherein the first component is further configured to store the first certificate.

19. The apparatus of Claim 16 further comprising a third component, coupled to the first component, and configured to generate the first certificate based, in part, on information provided by the client.

20. An apparatus for receiving authentication over a network, comprising:

a first component configured to generate a certificate;

a second component, coupled to the first component, configured to send the certificate to a server; and

a third component, coupled to the second component, configured to resend the certificate to the server over the network, wherein resending the certificate enables the server to authenticate the client based, in part, on a comparison of the sent certificate and the resent certificate.

21. The apparatus of Claim 20, wherein the apparatus operates as at least one of a client, a portable computer, and a personal digital assistant.

22. The apparatus of Claim 20, wherein the certificate is sent to the server using a trusted mechanism selected from at least one of a manual entry of certificate, a secure channel, and a private channel.

23. The apparatus of Claim 22, wherein the trusted mechanism further comprises at least one of the client authenticating to the server, and the client proving ownership of the certificate to the server.

24. A system for authenticating a client over a network, comprising:

a client, configured to perform actions, comprising:

generating a first certificate;

sending the first certificate to a server to be stored; and

sending a second certificate if authentication over the network is requested; and

a server, in communication with the client, configured to perform actions, comprising:

storing the first certificate at the server if the first certificate is received for a first time;

comparing the second certificate to the first certificate; and

authenticating the client over the network, if the first certificate and the second certificate are substantially the same.

25. The system of Claim 24, wherein authenticating the client over the network further comprises establishing a secure session.

26. A system for authenticating a client over a network, comprising:

a client, further comprising:

means for generating a first certificate;

means for sending the first certificate to a server to be stored; and

means for sending a second certificate if authentication over the network is requested; and

a server, in communication with the client, further comprising:

means for storing the first certificate at the server if the first certificate is received for the first time;

means for comparing the second certificate to the first certificate; and

means for authenticating the client, if the first certificate and the second certificate are substantially the same.

27. The system of Claim 26, wherein the means for storing comprises at least one of a hard disk, a tape disk, and a mass storage device.